

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

TIMOTHY CHEN *individually and on behalf
of all others similarly situated,*

Plaintiff,

v.

FLIGHTAWARE, LLC,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Timothy Chen (Plaintiff) brings this Class Action Complaint on behalf of himself and all others similarly situated, against Defendant FlightAware, LLC (“FlightAware” or “Defendant”), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to his, which are based on personal knowledge.

NATURE OF THE ACTION

1. This class action arises out of Defendant’s failures to implement reasonable and industry standard data security practices to properly secure, safeguard, and adequately destroy Plaintiff’s and Class Members’ sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant’s data security failures allowed a targeted cyberattack to compromise Defendant’s network (the “Data Breach”) that, upon information and belief, contained personally identifiable information (“PII” or “Private Information”) of Plaintiff and other individuals (“the Class”). The Data Breach occurred in or around July 2024.¹

3. Defendant, FlightAware is a provider of real-time and historical flight information

¹ A sample Notice of Security Incident posted to the California Attorney General’s Office is attached hereto as Exhibit A.

and insights to the global aviation community.²

4. Defendant, notified Plaintiff and Class members' of the Security Breach by posting a notice of Security Incident to the California Attorney General's Office stating³:

On July 25, 2024, we discovered a configuration error that may have inadvertently exposed your personal information in your FlightAware account, including user ID, password, and email address. Depending on the information you provided, the information may also have included your full name, billing address, shipping address, IP address, social media accounts, telephone numbers, year of birth, last four digits of your credit card number, information about aircraft owned, industry, title, pilot status (yes/no), and your account activity (such as flights viewed and comments posted). Additionally, our investigation has revealed that your Social Security Number may have been exposed.

5. The Private Information compromised in the Data Breach included certain personal information of individuals whose Private Information was maintained by Defendant, including Plaintiff.

6. Upon information and belief, a wide variety of PII was implicated in the breach, including, name, addresses, and Social Security numbers.⁴

7. Plaintiff and Class Members at no point knowingly provided their PII to Defendant and Defendant instead scraped their PII from non-public sources. To make matters even worse, Defendant did this without Plaintiff's and Class Members' consent or knowledge.

8. The mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

² See <https://www.linkedin.com/company/flightaware/about/> (last visited Aug. 21, 2024).

³ <https://oag.ca.gov/system/files/Notice%20to%20Data%20Subjects-%20CA.pdf> (last visited Aug. 21, 2024).

⁴ *Id.*

9. Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

10. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

11. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Private Information of Plaintiff and Class Members.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's

negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

13. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

14. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the Dark Web.

15. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

16. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive Private Information,

which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of fiduciary duty, (iii) breach of implied contract, (iv) violation of California's Unfair Competition Law, (v) violation of the California Consumer Privacy Act, (vi) Violation of the California Consumer Records Act, (vii) unjust enrichment.

19. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

20. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and insecure.

PARTIES

21. Plaintiff Timothy Chen is an individual who at all relevant times has been a citizen and resident of the State of California.

22. Plaintiff is a customer of Defendant's platform.

23. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

24. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

25. Plaintiff is not aware of ever being part of a data breach before, and is concerned that it and other private information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including checking his credit monitoring services, setting up notices and reports and carefully reviewing all his accounts.

26. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

27. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

28. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a

result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

29. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

30. Defendant FlightAware, LLC is a Texas corporation with its headquarters and principal place of business located at 11 Greenway Plz, Suite 2900, Houston, TX 77046-1111.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

32. This Court has personal jurisdiction over Defendant because it is a Texas corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims.

34. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

35. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

36. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

37. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."⁵

38. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.⁶

39. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped

⁵ Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/> (last visited Aug. 21, 2024).

⁶ *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, available at <https://notified.idtheftcenter.org/s/resource#annualReportSection>.

losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to \$1.7 billion in 2018.⁷

40. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

41. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."⁸

42. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

⁷ Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at [https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20\(1\)](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1)).

⁸ United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: <https://www.gao.gov/assets/gao-07-737.pdf>.

B. Defendant Breached its Duty to Protect Plaintiff and Class Members' PII

43. Defendant agreed to and undertook legal duties to maintain the protected personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Under state and federal law, businesses like Defendant have duties to protect its client's PII and to notify them about breaches.

44. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiff and Class Members.

45. In or around July 2024, Defendant became aware of a ransomware attack on its system.

46. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect Plaintiff and Class Member's PII.

C. Plaintiff and Class Members Suffered Damages

47. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

48. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

49. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

50. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.⁹

51. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹⁰

52. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect Plaintiff and Class Member's Private Information.

COMMON INJURIES AND DAMAGES

53. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

54. Due to the Data Breach, and the foreseeable consequences of Private Information

⁹ <https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud>.

¹⁰ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>.

ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) “out of pocket” costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant’s possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information.

A. The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

55. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

56. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

57. For example, armed with just a name and date of birth, a data thief can utilize a

hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

58. The dark web is an unindexed layer of the internet that requires special software or authentication to access.¹¹ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or ‘surface’ web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address is ciadotgov4sjwlzihbbgxngq3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.¹² This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

59. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.¹³ The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of

¹¹ *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

¹² *Id.*

¹³ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

birth, and medical information.¹⁴ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”¹⁵

60. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁶

61. What’s more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

¹⁴ *Id.*; *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

¹⁵ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

¹⁶ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

old bad information is quickly inherited into the new Social Security number.”¹⁷

63. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant being issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines.¹⁸

64. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.¹⁹

65. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”²⁰ Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

66. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

67. In addition to out-of-pocket expenses that can exceed thousands of dollars and the

¹⁷ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

¹⁸ *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

¹⁹ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.

²⁰ *Id.*

emotional toll identity theft can take, victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

68. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”²¹

69. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.²²

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

70. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this

²¹ Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

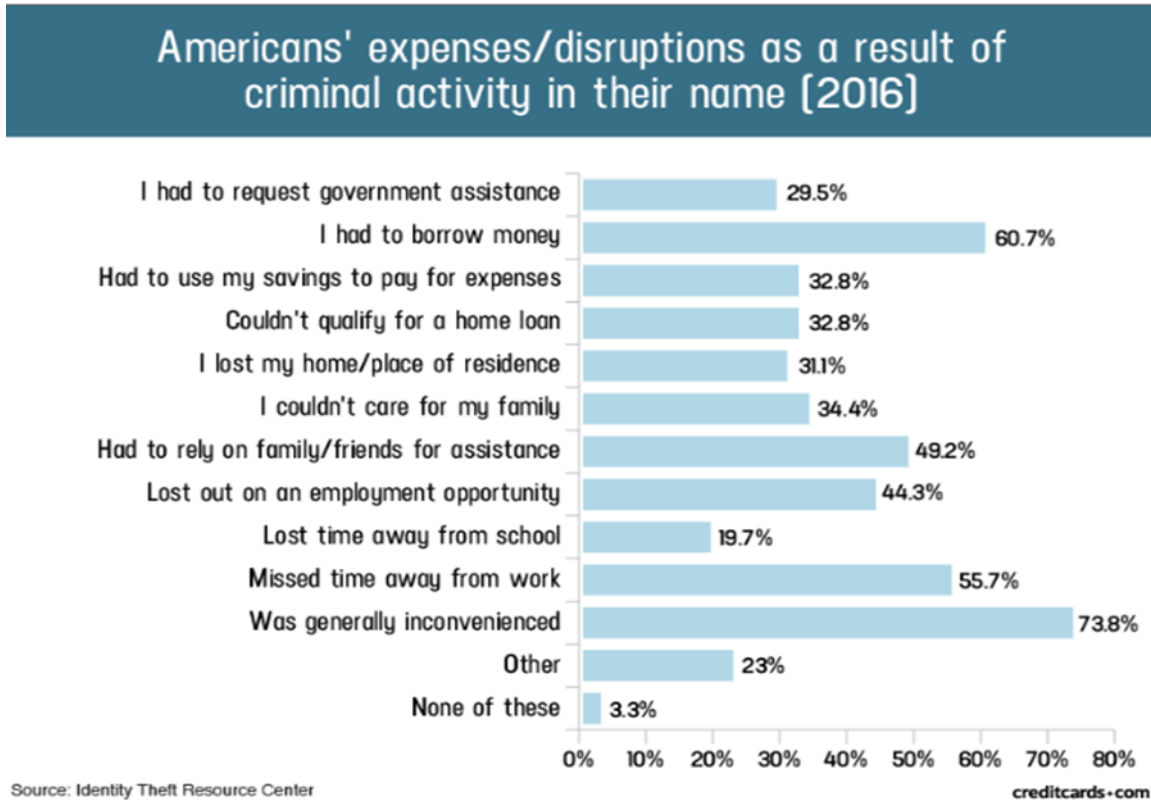
²² See generally <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

71. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

72. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²³

²³ “Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.



73. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁴ Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁵

²⁴ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

²⁵ See <https://www.identitytheft.gov/Steps>.

C. Diminution of Value of the Private Information

74. PII is a valuable property right.²⁶ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

75. Private Information can sell for as much as \$363 per record according to the Infosec Institute.²⁷

76. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.²⁸ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{29, 30} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50 a year.³¹

77. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

²⁶ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

²⁷ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

²⁸ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

²⁹ <https://datacoup.com/>.

³⁰ <https://digi.me/what-is-digime/>.

³¹ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

78. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any relief or protection. Furthermore, this is a tacit admission that its failure to protect their Private Information has caused Plaintiff and Class great injuries.³²

79. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach. *Id.*

80. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

81. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

82. Furthermore, the information accessed and disseminated in the Data Breach is

³² See <https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident> (last visited Aug. 21, 2024).

significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.³³ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

83. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

84. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant’s failure to safeguard their Private Information.

E. Injunctive Relief is Necessary to Protect Against Future Data Breaches

85. Moreover, Plaintiff and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

86. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, he suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their Private Information is used;

³³ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

- b. diminution in value of their Private Information;
- c. compromise and continuing publication of their Private Information;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identity theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen Private Information; and
- h. continued risk to their Private Information—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

G. Lack of Compensation

87. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

88. As a direct and proximate result of Defendant’s conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

89. Further, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also

incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

90. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- f. Placing “freezes” and “alerts” with credit reporting agencies;
- g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- h. Contacting financial institutions and closing or modifying financial accounts;
- i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

91. In addition, Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

92. Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person’s life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

93. Defendant’s delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and has not formally notified all victims. They have yet to offer an explanation of purpose for the delay.

CLASS ALLEGATIONS

94. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Class:

Nationwide Class: All individuals whose PII was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach.

California Subclass: All residents of California, Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “Class”).

95. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded

party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

96. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

97. **Numerosity.** The class described above are so numerous that joinder of all individual members in one action would be impracticable, if not completely impossible. On information and belief hundred if not thousands of individuals have been notified by Defendant of the Breach. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

98. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

- a. Whether Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' Private Information;
- c. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiff's and Class Members' Private Information, and breached its duties thereby;
- d. Whether Defendant breached its fiduciary duty to Plaintiff and the Class.
- e. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

f. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

g. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

99. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiff and Class Members information was stored by Defendant's software, each having their Private Information obtained by an unauthorized third party.

100. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

101. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiff and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

102. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

103. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

104. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

105. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

106. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

107. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

108. Defendant's duty also arose from Defendant's position as a service provider. Defendant holds itself out as a trusted data collector, and thereby assumes a duty to reasonably protect its customers' employees' information. Indeed, Defendant, as a direct data collector, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

109. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its clients.

110. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its customers.

113. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

114. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

116. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

- a. Theft of their Private Information;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. The erosion of the essential and confidential relationship between Defendant—as a services provider—and Plaintiff and Class members as customers; and

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Classes)

118. Plaintiff hereby repeat and reallege paragraphs 1 through 103 of this Complaint and incorporate them by reference herein.

119. Plaintiff and the other Class members gave Defendant their PII believing that Defendant would protect that information. Plaintiff and the other Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and the other Class members' PII created a fiduciary relationship between Defendant on the one hand, and Plaintiff and the other Class members, on the other hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiff's and the other Class members' PII.

120. Due to the nature of the relationship between Defendant and Plaintiff and the other Class members, Plaintiffs and the other Class members were entirely reliant upon Defendant to ensure that their PII was adequately protected. Plaintiff and the other Class members had no way of verifying or influencing the nature and extent of Defendant's or their vendors' data security policies and practices, and Defendant were in an exclusive position to guard against the Data Breach.

121. Defendant has a fiduciary duty to act for the benefit of Plaintiff and the other Class members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class members' PII, failing to comply with the data security guidelines set forth by HIPPA, and otherwise failing to safeguard Plaintiff's and the other Class members' PII that they collected.

122. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data breach; (vii) loss of potential value of their PII; (viii) overpayment for the services that were received without adequate data security.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Classes)

123. Plaintiff hereby repeat and reallege paragraphs 1 through 103 of this Complaint and incorporate them by reference herein.

124. Defendant offered to provide services to its customers, including Plaintiff and Class members, in exchange for payment.

125. Defendant also required Plaintiff and the Class members to provide their Private Information to receive services.

126. In turn, Defendant impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures.

127. Plaintiff and the Class members accepted Defendant offer by providing Private Information to Defendant in exchange for receiving Defendant services, and then by paying for and receiving the same.

128. Plaintiff and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

129. Defendant materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

130. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

131. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

132. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

133. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

FOURTH CAUSE OF ACTION
Violation of California's Unfair Competition Law (UCL)
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiff and the California Subclass)

134. Plaintiff hereby repeat and reallege paragraphs 1 through 103 of this Complaint and incorporate them by reference herein.

135. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts or practices (“UCL”).

136. Defendant’s conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the “CCPA”), and other state data security laws.

137. Defendant stored the PII of Plaintiffs and the California Subclass in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff’s and the California Subclass’s PII secure to prevent the loss or misuse of that PII.

138. Defendant failed to disclose to Plaintiffs and the California Subclass that their PII was not secure. However, Plaintiffs and the California Subclass were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiffs and the California Subclass on notice that their PII was not secure, which Defendant had a duty to disclose.

139. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs’ and the California Subclass’s nonencrypted and nonredacted PII.

140. Had Defendant complied with these requirements, Plaintiffs and the California Subclass would not have suffered the damages related to the data breach.

141. Defendant’s conduct was unlawful, in that it violated the CCPA.

142. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

143. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

144. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

145. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

146. Instead, Defendant made the PII of Plaintiffs and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

147. As a result of those unlawful and unfair business practices, Plaintiffs and the California Subclass suffered an injury-in-fact and have lost money or property.

148. For one, on information and belief, Plaintiffs' and the California Subclass's stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

149. The injuries to Plaintiffs and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

150. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

151. Therefore, Plaintiffs and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

FIFTH CAUSE OF ACTION
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff and the California Subclass)

152. Plaintiff hereby repeat and reallege paragraphs 1 through 103 of this Complaint and incorporate them by reference herein.

153. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs and the California Subclass's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

154. Defendant is a “business” under the meaning of Civil Code § 1798.140 because Defendant is a “corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners” that “collects consumers’ personal information” and is active “in the State of California” and “had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year.” Civil Code § 1798.140(d).

155. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs and California Subclass members’ PII. Plaintiffs and California Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

156. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice letter to Defendant’s registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

157. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

158. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

SIXTH CAUSE OF ACTION
Violation of the California Consumer Records Act

Cal. Civ. Code § 1798.80, et seq.
(On behalf of Plaintiff and the California Subclass)

159. Plaintiff hereby repeat and reallege paragraphs 1 through 103 of this Complaint and incorporate them by reference herein.

160. Under the California Consumer Records Act, any “person or business that conducts business in California, and that owns or licenses computerized data that includes personal information” must “disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82. The disclosure must “be made in the most expedient time possible and without unreasonable delay” but disclosure must occur “immediately following discovery [of the breach], if the personal information was, *or* is reasonably believed to have been, acquired by an unauthorized person.” *Id* (emphasis added).

161. The Data Breach constitutes a “breach of the security system” of Defendant.

162. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the California Subclass.

163. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Subclass but waited approximately 254 days to notify them. Given the severity of the Data Breach, 254 days was an unreasonable delay.

164. Defendant’s unreasonable delay prevented Plaintiffs and the California Subclass from taking appropriate measures from protecting themselves against harm.

165. Because Plaintiffs and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

166. Plaintiffs and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

SEVENTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

167. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

168. Plaintiff brings this claim in the alternative to his breach of third-party beneficiary contract claim above.

169. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiff's and Class Members'.

170. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as a necessary part of their obtaining automobile's at Defendant's clients. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

171. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

172. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

173. Defendant, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

174. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

175. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

176. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

177. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

178. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because

Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

179. Plaintiff and Class Members have no adequate remedy at law.

180. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

181. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

182. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling

personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: August 26, 2024

Respectfully Submitted,

/s/Andrew J. Shamis
Andrew J. Shamis
Texas Bar No. 24124558
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Tel: 305-479-2299
ashamis@shamisgentile.com

Counsel for Plaintiff and the Putative Class